11

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,742	07/31/2001	Ernst-Michael Hamann	DE920000056US1	2722

7590 07/01/2005

Jeanine S. Ray-Yarletts
IBM Corporation
T81/503
PO Box 12195
Research Triangle Park, NC 27709

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

47

Office Action Summary	**Application No.** 09/918,742	**Applicant(s)** HAMANN ET AL.	
	Examiner Kevin Schubert	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 27 May 2005.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 7,9,12,13 and 16 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 7,9,12,13 and 16 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claims 7,9,12-13, and 16 have been considered.

Claim Objections

Claim 9 is objected to because of the following informalities: the phrase "comprising the:" should be replaced with "comprising:". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 9 and 12 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. In part d of claim 9, the applicant claims "signing said user certificate with said digital signature when both HASHs are identical". "Said digital signature" refers to the digital signature of the root certifying authority which is placed on the certificate using a private key of the root certifying authority. This is the case because the public root key is needed to decrypt the digital signature. However, comparison of the HASHs is done at the security token, or client, site. Thus, the claim is not enabled because the security token, or client, site would not have the private key of the root certifying authority. Therefore, the security token, or client, site could not sign the user certificate when both HASHs are identical.

Claims 9 and 12 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. In part d of claim 9, "signing said user certificate with said digital signature when both HASHs are identical" is not disclosed by the Specification. The Specification discloses signing a message with a user private key, but the Specification does not disclose signing a certificate or the use of creating a digital signature of a root certifying authority when the generated HASH and the decrypted HASH are identical.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 7 and 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In part e, the applicant claims "verifying a digital signature of the certificate authority stored in the security token". It is unclear whether the applicant is claiming that a digital signature is stored in the security token or a certification authority is stored in the security token. The examiner assumes the applicant meant that a digital signature is stored in the security token. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 7 and 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Geiger, U.S. Patent No. 6,463,534.

As per claims 7 and 16, the applicant describes a method comprising the following limitations which are met by Geiger:

a) transferring a root certificate of a certification authority into said security token using a secure transmission environment (Col 5, lines 3-10);

b) securing the root certificate against modifications (Col 5, lines 3-10);

c) storing a verification component into said security token allowing use or replacement of a user certificate only when said user certificate is authenticated by said root certificate (Col 6, lines 5-25);

d) creating a user digital signature in the security token using a private key assigned to the security token (Col 17, lines 36-41);

e) wherein said authentication by said root certificate further comprises verifying a digital signature of the certification authority stored in the security token using a public root key of the certification authority (Col 6, lines 20-25);

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 7,9,12, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogel, U.S. Patent No. 6,816,900 in view of Epstein, U.S. Patent No. 6,694,025, in further view of Geiger.

As per claims 7,9, and 16, the applicant describes a method for initializing a security token for a mobile device comprising the following limitations which are met by Vogel, Epstein, and Geiger:

a) transferring a root certificate of a certification authority into said security token using a secure transmission environment (Vogel: Col 2, lines 15-19);

b) securing the root certificate against modifications (Vogel: Col 2, lines 15-19);

c) storing a verification component into said security token allowing use or replacement of a user certificate only when said user certificate is authenticated by said root certificate (Vogel: Col 2, lines 38-52);

d) creating a user digital signature in the security token using a private key assigned to the security token (Epstein: Col 5, lines 51-55);

e) wherein said authentication by said root certificate further comprises verifying a digital signature of the certification authority stored in the security token using a public root key of the certification authority (Vogel: Col 8, lines 50-60);

Vogel does not disclose that the computing device has the capability to create signatures. Epstein discloses a system in which a computing device requests the creation of a private key from a server and is assigned a private key which is maintained at a server (Col 5, lines 23-33). When the user wants to sign something using his assigned private key, the user requests the private key from the server, receives the private key, and makes a signature. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Epstein with Vogel because doing so allows a user to create a digital signature.

Vogel in view of Epstein disclose that the device which receives the certificates is computing device, but not necessarily that the device is a mobile device. Geiger discloses the idea that a mobile device can receive certificates and store them in a security token, such as a smart card (Col 11, lines 64-67; Fig 4). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Geiger with those of Vogel in view of Epstein and have the computing device be a mobile device because doing so provides portability.

As per claim 12, the applicant describes a method according to claim 9, which is met by Vogel in view of Epstein in further view of Geiger, with the following limitation which is met by Vogel:

Checking the validity of the root certificate before retrieving said public root key (Vogel: Col 10, lines 1-10).

Claim 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogel in view of Aucsmith, U.S. Patent No. 6,175,626, in further view of Geiger.

As per claim 13, the applicant describes a method for replacing a user certificate stored in a security token in a mobile device comprising the following limitations which are met by Vogel in view of Aucsmith in further view of Geiger:

a) receiving a new user certificate from a certification authority and storing it into said security token as a temporary object (Vogel: Col 7, line 64 to Col 8, line 17; Col 10, lines 66-67);

b) generating a HASH over the new user certificate using a HASH algorithm specified in said new user certificate (Vogel: Col 7, lines 64 to Col 8, line 17);

c) retrieving a digital signature contained in said new user certificate and decrypting said digital signature by applying a public root key retrieved from a certification authority root certificate resulting in a HASH of said user certificate (Vogel: Col 7, line 64 to Col 8, line 17; Aucsmith: Col 12, lines 41-44);

d) permanently storing said new user certificate in the security token when both HASHs are identical (Vogel: Col 7, line 64 to Col 8, line 17).

Vogel discloses a system in which a user receives a new certificate to store in his root certificate store. The process of updating the new certificates on the user's computing device takes place via an update root control which can on the computing device (Col 10, lines 66-67). The update root control receives a signed message which contains user root certificates to store in the user's root certificate store. The signed message with the certificates is received by the update root control and held as a temporary object in the update root control (part a). When validation occurs by matching a generated HASH of the certificate with the HASH value in the signed message, the certificate is then permanently stored in the root certificate store of the computing device, or security token (parts b and d).

Vogel discloses a HASH matching process in which the first HASH is generated by using a HASHING algorithm. However, in Vogel's system the second HASH is retrieved from the message, not decrypted from the digital signature on the certificate. Aucsmith discloses the well-known idea that a

HASH of a certificate can be retrieved by using the public key of the signer found on a certificate to decrypt the signature. Combining Aucsmith would simply mean that instead of retrieving the second HASH value from the HASH values of the signed message, the HASH value is retrieved by decrypting the digital signature on the certificate. Furthermore, since the received user certificate is a root certificate, the user would be applying a public root key retrieved from a certification authority root certificate to create the second hash.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Aucsmith with those of Vogel because doing so provides an extra authentication step and more security in the system. This would be an obvious combination in the case where the security of providing an extra authentication step of decrypting the signature is more important than the convenience of simply retrieving the HASH value.

Vogel in view of Aucsmith disclose that the device which receives the certificates is computing device, but not necessarily that the device is a mobile device. Geiger discloses the idea that a mobile device can receive certificates and store them in a security token, such as a smart card (Col 11, lines 64-67; Fig 4). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Geiger with those of Vogel in view of Aucsmith and have the computing device be a mobile device because doing so provides portability.

Response to Arguments

Applicant's arguments, see Remarks filed 5/27/05, with respect to parts c and e of claim 7 have been fully considered but they are not persuasive. The applicant argues that Geiger does not disclose a technique for verifying a digital signature of the certification authority in the security token. The examiner disagrees. Geiger discloses that certificates stored in the security token are verified every time the mobile device is booted up (Col 6, lines 5-25). Specifically, Geiger teaches the following passage: "the phone's boot software compares the digital signature of the certificates with the CA's Public Key Certificate (which was installed in the factory) to ensure that forged certificates were not installed (Col 6, lines 22-25). The examiner notes that the CA's Public key certificate which contains the public key used to verify the digital signatures of the certificates is a root certificate (Col 5, lines 3-6). Thus, Geiger does disclose a verification component allowing use of a certificate (part c) and verifying a digital signature of the certification authority (part e).

Applicant's arguments with respect to claim 9 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection has been made.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100